Enabling Strong Authentication with Personal Identification Verification Cards: Public Key Infrastructure (PKI) in Enterprise Physical Access Control Systems (E-PACS) Recommended Procurement Language for RFPs

VERSION **Release Candidate 2**

FICAM TESTING PROGRAM

June 28, 2013

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	6/12/2013	Initial draft	Limited
Draft	0.0.1x	6/19/2013	First team edit	Limited
Draft	0.0.2	6/20/2013	Second team edit	Limited
Draft	0.0.3	6/20/2013	Edit for distribution w/in team	Limited
Draft	0.0.4	6/21/2013	Full team edit	Limited
Draft	0.0.5	6/22/2013	QA	Limited
Draft	RC1	6/24/2013	Review/Accept QA	Limited
Draft	RC2	6/24/2013	Updates per senior review team	Limited

Table of Contents

1 Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard 201 [FIPS 201] Evaluation Program (EP) and its FIPS 201 Approved Products List (APL), as well as services for Federal Identity, Credentialing and Access Management (FICAM) segment architecture conformance and compliance. GSA is currently transitioning the FIPS 201 EP and APL into the enhanced GSA FICAM Testing Program.

The GSA FICAM Testing Program provides testing of Enterprise Physical Access Control Systems (E-PACS) for listing on the APL that fully support both Personal Identity Verification (PIV) and PIV Interoperable (PIV-I) credentials. Performance based requirements for the use of PIV and PIV-I in E-PACS are detailed in the FICAM Testing Program *Functional Requirements and Test Cases* [FRTC] document.

Office of Management and Budget (OMB) Memorandum M-06-18 [M-06-18] requires the use of the APL in all procurements:

> "Agencies that proceed with the acquisition of products and services for the implementation of HSPD-12 through acquisition vehicles other than GSA IT Schedule 70 must ensure that only approved products/services from the Approved Product List are acquired and incorporated into system solutions and ensure compliance with other federal standards and requirements for systems used to implement HSPD-12. In order to ensure government-wide interoperability, this applies for the lifecycle of the products, services, and/or systems being acquired."

OMB Memorandum M-11-11 [M-11-11] requires that all acquisitions be compliant with the *FICAM Roadmap and Implementation Guidance* [FICAM Roadmap] and that all E-PACS acquisitions be compliant with *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116* [SP 800-116]. Specifically:

> To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:
>
> - Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.
> - Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using

development and technology refresh funds to complete other activities.

- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.
- Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.
- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov).

2 Intended Audience

This document is intended for use by procurement officials in developing Requests for Proposals, Statements of Work, and/or Performance Work Statements for the acquisition of HSPD-12, FIPS 201 and FICAM conformant E-PACS solutions for use in federal facilities. Individuals involved in developing procurements may include Contract Officers, Contracting Officer Technical Representatives, Facility Security Professionals and System Architects.

3 Objectives

This document provides language for PACS related procurements to ensure compliance with applicable policies noted above. This language is intended to be added to the requirements section of the SOW or RFP. The language fully leverages approved Public Key Infrastructure (PKI) authentication methods for E-PACS listed on the APL. The language is fully conformant with the mandates within [M-11-11] to stay aligned with [FICAM Roadmap] and [SP 800-116].

The procurement language provided is tightly focused on requiring all E-PACS solutions to be capable of supporting approved PKI authentication methods. This language does not provide architectural guidance, implementation detail or limitations on use of additional authentication methods. Program Managers and System Architects writing

RFP/SOW language may find useful guidance in the FICAM PIV in E-PACS Guidance Draft Version 2.1, January 31, 2013[1].

4 Recommended Language for E-PACS RFPs and SOWs

All Request for Proposals (RFP) and Statements of Work (SOW) for new or upgraded E-PACS should include the language for integrating the mandatory authentication mechanisms of [FIPS 201] into E-PACS provided in both *Section 4.1* and *Section 4.2*. The section headers and language are designed to be directly cut and pasted into procurements. As such, these section state requirements and shalls for direct inclusion into procurements. Please note that the normative references in *Section 4.2* support the language in *Section 4.1* and may be in addition to any other normative references required by the procurement.

[1] The FICAM PIV in E-PACS document can be found on http://idmanagement.gov/ficam-testing-program. The specific download URL ishttp://idmanagement.gov/documents/piv-e-pacs.

4.1 Requirements for PKI in E-PACS

Office of Management and Budget (OMB) Memorandum M-06-18 [M-06-18] requires all agencies to use the General Services Administration (GSA) Approved Products List (APL) in all procurements for *Homeland Security Presidential Directive 12* [HSPD-12] and Federal Information Processing Standard 201 [FIPS 201] compliant systems. The GSA Federal Identity, Credential, and Access Management (FICAM) Testing Program lists compliant Enterprise Physical Access Control Systems (E-PACS) solutions on the GSA APL for procurements.

OMB Memorandum M-11-11 [M-11-11] requires all E-PACS systems at federally owned or leased buildings "be enabled to use PIV credentials" and that "agency processes must accept and electronically verify PIV credentials issued by other federal agencies." [M-11-11] further requires compliance with FICAM Roadmap and Implementation Guidance [FICAM Roadmap], which expands the use of Personal Identity Verification (PIV) to include PIV Interoperable (PIV-I) credentials in FICAM compliant solutions. Both PIV and PIV-I credentials contain PKI digital certificates, fingerprint minutia templates, and a secure Personal Identity Number (PIN).

"Electronically verify" means that the E-PACS at federally owned or leased facilities must be capable of performing ***PKI strong authentication methods*** to establish a high degree of confidence in the binding between the credential and the bearer. Before granting physical access to a Government employee or contractor who has been issued a PIV or PIV-I credential, the E-PACS must evaluate the credential to determine:

1. The digital certificate is valid at time of use (e.g., has not been placed on the certificate revocation list (CRL) within the previous 6 hours),
2. A successful challenge/response was issued utilizing the private key, and
3. A positive confirmation that the certificate's public key is identical to the public key authorized to access the facility.

Depending on the local security level, E-PACS shall support a minimum of one FICAM approved PIV PKI authentication method, specifically PKI-CAK, PKI-AUTH, and PKI-AUTH + BIO(-A), as defined in [SP 800-116] in accordance with ICAM SC Guidance. The systems must be comprised of products that are listed on the APL. As required by FIPS 201, PACS must validate that PIV Credentials were issued under [COMMON] and have not been placed on a CRL more than 6 hours before the time of access.

1. Contractor shall ensure that proposed solutions align with these goals and fully describe related capabilities, assumptions, limitations, and non-conformance.
2. Any non-conformance to this requirement must be justified in a separate technical appendix. This appendix may be shared with the ICAM SC and the FIPS 201 EP.

The E-PACS shall be capable of evaluating the validity of a PIV/PIV-I credential and the binding of the credential to the bearer at time of registration and at time of access in accordance with the following requirements:

1. The E-PACS shall confirm the validity of the PIV/PIV-I credential presented by performing the following functions:
   a. Active Authentication
      i. A challenge/response protocol using PKI certificates on the PIV/PIV-I card.

ii. *Note:* at time of access, the E-PACS shall confirm the public key used in item 1.a.i is identical to the public key that was initially registered for access.

b. Validation of Trusted Origin
   i. Certificate status checking (i.e. confirming expiration, revocation, signature validation).
   ii. Path discovery and validation (i.e. evaluating the full trust chain to a trust anchor for policies, constraints, revocation status and signature verification).
   iii. The certificate policy presented by the credential shall chain back to [Common] for PIV, or to [FBCA] for PIV-I.

c. Bearer Confirmation
   i. Use PKI-CAK with no additional requirement for bearer confirmation.
   ii. Use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
   iii. Use PKI-AUTH + BIO(-A) for challenge/response and confirmation of the bearer's presented PIN and fingerprint.

Only when the results of these three operations (1.a, 1.b and 1.c) are confirmed as positive should a credential either be registered to the E-PACS for authorization, or granted access based on the authorization profile for that credential.

2. The E-PACS shall use one or a combination of the following to perform item 1.b "Validation of Trusted Origin":
   a. Certificate Revocation Lists (CRLs),
   b. Online Certificate Status Protocol (OCSP), or
   c. Server-based Certificate Validation Protocol (SCVP).
3. The E-PACS may use cached information for item 1.b "Validation of Trusted Origin". In all cases, credentials must be valid at time of registration or access. It is recommended that:
   a. Revocation status should not be more than 6 hours old.
   b. Full path discovery and validation information should not be more than 18 hours old.
4. At time of in-person registration, the E-PACS shall:
   a. Capture the Content-Signer certificate, the PKI-AUTH certificate, and the PKI-CAK certificate for purposes of periodic Validation of Trusted Origin (items 1.b, 2 and 3).
   b. At a minimum, use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
   c. Check the expiration date of all data objects and signers on the credential and perform a private key challenge/response for each certificate being registered.
   d. Perform Verification of Trusted Origin of the user's credential and its signers.
5. An organization may have an Enterprise Identity Management (E-IdM) system in place. In this environment, the E-PACS may have direct provisioning and de-provisioning of access records from the E-IdM that are tightly bound to Human Resources processes. This method shall be in addition to "Verification of Trusted Origin" as described in items 1.b, 2 and 3.

a. At a minimum, the E-IdM shall provide the CHUID, the Content-Signer certificate, the PKI-AUTH certificate, and the PKI-CAK certificate for purposes of periodic "Verification of Trusted Origin" (items 1.b, 2 and 3).

4.2 Normative References

[HSPD-12]	Homeland Security Presidential Directive 12, August 27, 2004
[FIPS 201]	Federal Information Processing Standard (FIPS) 201 Personal Identity Verification, March 2006
[M-06-18]	Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
[M-11-11]	Office of Management and Budget (OMB) Memorandum M-11-11, February 3, 2011
[FICAM Roadmap]	FICAM Roadmap and Implementation Guidance
[SP 800-116]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116
[FRTC]	FICAM Testing Program Functional Requirements and Test Cases
[Common]	FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.17, December 9, 2011
[FBCA]	FBCA X.509 Certificate Policy For Federal Bridge Certification Authority (FBCA), Version 2.25, December 9, 2011